AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: /S Bow Bottomly 06/27/2024

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of *(Briefly describe the property to be search* *Or identify the person by name and address)* PROPERTY KNOWN AS: 1. SanDisk 128 GB SD card IN THE POSSESSION OF: HSI Oklahoma City 3526 NW 56th St Oklahoma City, OK 73112	)	Case No: M-24-533-STE

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

18 U.S.C. § 2251	Production of Child Pornography
18 U.S.C. § 2252A	Distribution and Possession of Child Pornography
18 U.S.C. § 1591(a)	Sex Trafficking of Children

The application is based on these facts:

See attached Affidavit of Special Agent Nicholas Ustach, Homeland Security Investigations, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

Nicholas Ustach
Special Agent
Homeland Security Investigations

Sworn to before me and signed in my presence.

Date: June 27, 2024

City and State: Oklahoma City, Oklahoma

Shon T. Erwin

Judge's signature

SHON T. ERWIN, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Nicholas Ustach being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since September 11, 2022. I spent six months at the Federal Law Enforcement Training Center completing the Criminal Investigator Training Program and HSI Special Agent Training Programs. I previously spent four years employed with US Customs and Border Protection. In the course of my duties, I was exposed to many human and drug smuggling incidents, interviewed parties applying for admission at the Port of Entry, performed searches of vehicles and persons, and processed immigration cases that presented themselves at the port. I participated in multiple discoveries of drugs concealed within vehicles, merchandise, and on persons and performed seizures of the drugs. Before that, I received a Bachelor of Science in Sociology from Brigham Young University and a Master of Science in Criminal Justice from Weber State University.

2. I am currently assigned to HSI Oklahoma City, Oklahoma. As part of my duties, I am tasked with investigating federal criminal cybercrime violations. I have both training and experience conducting child exploitation and child pornography investigations. Moreover, I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators. I have become aware of numerous examples of child pornography (as

defined in 18 U.S.C. § 2256) in all forms of media, to include electronic media.

3. The statements contained in this affidavit are based in part on information provided by law enforcement officials and others known to me, and on my own experience and background as a law enforcement officer. Since the affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of Title 18 U.S.C. §§ 2251 and 2252A(possession, distribution, and production of child pornography), and Title 18 U.S.C. § 1591(a)(sex trafficking of children) have been committed and that the instrumentalities, fruits, and evidence of those crimes will be found in a particular place to be searched.

4. This affidavit is made in support of a search warrant for the following items ("DEVICES"), which are currently in the legal custody of Homeland Security Investigations, Oklahoma City, and located in their secure evidence storage room at 3625 NW 56th St, Oklahoma City, Oklahoma:

a. Apple iPad with Black Case

b. Apple iPad with Grey Case

c. Blue Motorola Cell Phone

d. Apple iPhone with Grey Case

e. Apple iPhone with Purple Case

f. Apple iPhone with Green Case

g. Apple SanDisk 128 GB SD Card

I am submitting this affidavit in support of a search warrant authorizing a search of the DEVICES (also described in Attachment A to this affidavit) and the extraction from the DEVICES of electronically stored content and information described in Attachment B hereto, which content and information constitute instrumentalities, fruits, and evidence of the foregoing violation.

5. This court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States. . . that has jurisdiction over the offense being investigated." 18 U.S.C. §2711(3)(A)(i), and "is in . . . a district in which the provider . . . is located or in which the wire or electronic communication, records, or other information are stored." 18 U.S.C. §2711(3)(A)(ii).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes

any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

j. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

k. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

n. A "storage medium" or "storage device" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

o. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

p. A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-

Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

PROBABLE CAUSE

7. On February 26, 2024, the Oklahoma Bureau of Narcotics (OBN) was contacted by Oklahoma Juvenile Affairs (OJA), stating that they believed they had a minor in their custody (herein identified as "MV") that was a victim of minor sex trafficking prior to arriving to their facility.

8. On February 27, 2024, an advertisement was located on a known commercial sex website, megapersonals.ue, with pictures of a person matching the description of MV. The advertisement listed the phone number (405) 761-8879 and said, "Hi, down to earth, submissive girl, loves to please, and give massages Hit me up ASAP, I will be waiting!" The advertisement was posted three times from January 17, 2024, to January 19, 2024, in Oklahoma City. The phone number was also listed in the advertisements for six other females in the Oklahoma City area on megapersonals.eu, with dates ranging from November 9, 2023, to February 13, 2024. All six profiles had the same title and description.

9. On March 21, 2024, OBN received a subpoena return for a request for subscriber information from T-Mobile for the phone number (405) 761-8879. According to T-Mobile, the subscriber of the phone number was Marlon MARTIN, with an address of 3214 S Walker Ave, Oklahoma City, Oklahoma 73109-6333, with an Account Effective Date of August 17, 2023.

10. On April 17, 2024, after an interview of MV, a state search warrant was executed on MV's cell phone. Upon extraction of the phone data, text conversations between MV and phone number (405) 761-8879, with a contact name of "Tatman", were found. Within the messages, MARTIN was seen arranging commercial sex dates for MV and notified MV of how much money needed to be collected from various suitors. MARTIN also indicated that he was close by during these dates and asked MV how long they were in hotel rooms with customers. In one conversation, MARTIN asked MV "When u turning 17" to which MV responds "April ayyyyy", indicating that MARTIN was aware of MV's age. Many text conversations with phone number (405) 906-0027 were also found during a review of MV's phone data extraction. The contact's name for the phone number was listed as "Tatman Marlon".

11. On May 28, 2024, OBN received a subpoena return for a request for subscriber information from T-Mobile for phone number (405) 906-0027. According to T-Mobile, the subscriber of the phone number was Marlon MARTIN, with an address at 3214 S Walker Ave, Oklahoma City, Oklahoma 73109-6333, with an Account Effective Date of August 17, 2023. The account had an Activation Date of August 28, 2019.

12. When reviewing text conversations between MV and MARTIN's 0027 phone number, the conversations showed MARTIN arranged multiple commercial sex dates for MV, arranged prices, collected money, and gave MV an alias to use. MV used

MARTIN's first name multiple times throughout the text messages. MARTIN stated he was paying for the hotel room MV was using for these dates.

13. Within the data extraction of MV's phone, photos and videos were discovered being sent between MARTIN and MV. On January 16, 2024, MARTIN sent a video of MV performing oral sex on an unknown black male from the (405) 906-0027 number to MV. Additionally, on January 18, 2024, MARTIN sent MV a picture of an unknown black male's penis from the same phone number. Evidence indicates the black male in the video and picture may be MARTIN.

14. In another text conversation found within MV's phone data extraction, MV was found to be texting a potential suitor for commercial sex. MV told the suitor to come to room 217 at a Motel 6 at 1337 SE 44th Street, Oklahoma City, OK, 73129. On May 28, 2024, OBN spoke with a clerk at that Motel 6 that confirmed that MARTIN had paid for room 217 from January 8 through 21, 2024, and had provided a driver's license for the reservation information. A copy of the room registration was provided to OBN that listed Marlon MARTIN as the guest with an address of 3214 S Walker Ave, Oklahoma City, OK, 73109. In remarks left by the hotel staff, it stated that MV was the second registered guest in the room.

15. On June 14, 2024, OBN obtained a state search warrant for MARTIN's residence at 3214 S Walker Ave, Oklahoma City, OK, 73109 to search for evidence of Human Trafficking, Pandering, Maintaining a House of Prostitution, Distributing Child

Pornography, and Using Access to Computers to Violate Oklahoma Statutes. On June 17, 2024, OBN, with assistance from HSI Oklahoma City, executed the search warrant at MARTIN's residence. MARTIN was present at the residence when it was searched. He was briefly interviewed. Among the evidence seized from the residence were the DEVICES, which are also described in Attachment A.

16. The DEVICES are currently in storage at the Homeland Security Investigations, Oklahoma City, secure evidence storage room at 3625 NW 56th St, Oklahoma City. In my training and experience, I know that the DEVICES have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICES were seized from MARTIN.

COMMON PRACTICES OF PERSONS WHO UNLAWFULLY ENGAGE IN SEX TRAFFICKING

17. Based on my training and experience, as well as the collective training, experience, and information from other law enforcement officials, I know the following:

a. Persons who perform sex work for value—sex workers—are often trafficked by someone known as a "pimp" or "madam." The pimp and sex worker represent the supply side of sex trafficking. The buyer seeking and paying for commercial sex represents the demand side of sex trafficking.

b. In most circumstances, the pimp is a third party who offers to provide physical protection for the sex worker and assist the sex worker in advertising her services and making sure she has food, shelter, and transportation to the locations where the

unlawful commercial sexual activity is to occur. When a pimp is involved, the sex worker typically gives all of the proceeds she earns from commercial sex to the pimp. A pimp typically utilizes various methods of control—both psychological and physical—to ensure compliance. However, sex trafficking also occurs when parents or guardians act as a pimp to sell their children to others for sex. Many times, those situations arise when parents or guardians have a history in the sex trade and/or have drug or alcohol dependencies and exploit their children to satisfy their addictions.

c. Sex traffickers almost always rely upon cellular telephones and computers to facilitate their business. Persons engaging in sex trafficking frequently communicate through text messaging, social media, email, and voice communications via cellular phones. Additionally, sex traffickers use the same methods of communication to recruit and control victims, advertise, connect between supply and demand, dispatch sex workers to meet with potential buyers, discuss prices, meeting arrangements, communicate threats or promises to victims and buyers, and arrange for the acquisition, transportation, and laundering of proceeds generated from these illegal activities. They frequently maintain text messages, social media messages, and voice communications for long periods of time. In many cases, a sex trafficking victim will have a phone with her for a commercial sex transaction with an open and live call with the pimp, who listens to and monitors the encounter. In many instances, sex workers will use internet- and social media-based telephone numbers.

d. Traffickers and sex workers/victims frequently take and store photographs and video recordings on their cellular devices and/or computer and transmit those photos and videos via social media applications and the internet. These photographs often include photographs of the sex workers/victims, both sexually explicit and non-explicit, that can be posted as advertisements for unlawful commercial sexual activity. Buyers and sex workers frequently exchange photos for identification purposes, and supply-side participants frequently document their proceeds from unlawful commercial sex activities in what are referred to as "trophy photos." These photos/videos also often include other sex workers, pimps, buyers and/or their associates.

e. Those that conspire or conduct transactions relating to human trafficking and/or unlawful commercial sex often identify themselves by monikers, street names, and/or nicknames to hinder law enforcement's efforts in identifying those involved with the commercial sex.

f. Sex workers and traffickers—both pimps and buyers—will often use coded words and phrases and vague conversations to discuss their plans and prevent anyone from overhearing their conversations and from recognizing that the conversations concern a commercial sex act.

g. A prospective buyer will often call or send a message to the sex worker to obtain permission to come to a location, i.e. hotel, residence, etc., to engage and/or solicit in the sexual encounter. The individuals typically use coded language to

discuss what they are seeking and offering. For example, payment is frequently described as a "donation," and dollars are sometimes called "roses." Other codes are used to discuss specific sex acts, but agreements are generally reached based on the increment of time—a quick visit (qv), half hour (hh), or full hour (hr).

h. Sex trafficking victims and sex workers are frequently advertised on a variety of social media platforms. These websites, applications, and platforms are often accessed by smartphones, cell phones, computers, and other similar devices.

BACKGROUND REGARDING COMPUTERS, CELLULAR PHONES, THE INTERNET, AND EMAIL

18. Based on information received from other law enforcement officials, I know the following:

a. Cell phone technology has revolutionized the way in which sex traffickers facilitate sex trafficking of adults and children, by connecting seller and buyer traffickers with victims and each other.

b. The development of various types of cell phones has added to the methods used by human traffickers to interact with and sexually exploit children. Cell phones—particularly "smart phones," or phones that have significant computing power, are usually connected to the internet, and often have digital cameras—may serve several functions in connection with human trafficking of children to include production and distribution of the child victims' images for elicit advertisement purposes, communication facilitating child sexual exploitation, and storage of the aforementioned.

c. As is the case with most digital technology, communications by way of a cell phone can be saved or stored on the cell phone used for these purposes, and even small devices can store tremendous amounts of data. Storing this information can be intentional, i.e., by saving an email as a file on the device or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, cell phone user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. I know that digital evidence, including pictures and videos, generally remains indefinitely on a digital storage device such as a cell phone until deleted or overwritten. I also know that even if a cell phone user deletes such evidence, a computer forensic expert can sometimes still recover it from the device using forensic tools months, and even years, after the fact.

19. Consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES as described in Attachment A and Attachment B. Such examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Law enforcement personnel (who may include, in addition to law enforcement officers and

agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review any data seized pursuant to the requested warrant to locate any evidence, fruits, and instrumentalities of child sex trafficking.

20. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

COMPUTERS, THE INTERNET AND CHILD PORNOGRAPHY

21. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures

have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (*i.e.*, "instant messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at

very high resolution. Given the storage capabilities, modern computers can retain many years' worth of a user's data, stored indefinitely. Even deleted data can often be forensically recovered. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person or in their immediate vicinity. Digital files can be quickly and easily transferred back and forth between computers (as broadly defined by 18 U.S.C. § 1030(e)) and other digital file storage devices or stored simultaneously on them. For example, smartphones can often synch with a traditional desktop or laptop computer. This can result in files being transferred from the smartphone to the computer or even stored on both devices simultaneously. Thus, I am requesting to seize and copy all electronic storage media on the DEVICES and search them.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous

fashion. For example, distributors of child pornography can use membership-based/subscription-based Web sites to conduct business, allowing them to remain relatively anonymous.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can usually be found on the user's computer or external media.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally: the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until

overwritten by other data. Thus, if a user has downloaded image files, viewed them, then deleted them, a computer forensic examiner could oftentimes find evidence of such actions and maybe even the deleted images themselves.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

22. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user

can conceal text in an image file, which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

23. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

24. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or

unsecured wireless network in their residence are often among the primary users of that wireless network.

25. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying all computers and electronic storage media on the DEVICES that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

26. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, possess, and/or collect child pornography:

a. Child pornography collectors usually start collecting child pornography by obtaining free images and videos of child pornography widely available on the internet on various locations and then escalate their activity by proactively distributing images they have collected, often for the purposes of trading images of child pornography with others, as a method of adding to their own collection of child

pornography.

b. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

c. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

d. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years. Collectors prefer not to be without their child pornography for any prolonged time period.

e. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence,

inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the collector to view the collection, which is valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

f. Child pornography collectors also may correspond with and/or meet others to share information and materials; keep correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[1]

Even if MARTIN uses a portable device (such as a mobile phone or Ipad) to access the Internet and child pornography, it is more likely than not that evidence of this access will

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

be found in his home, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

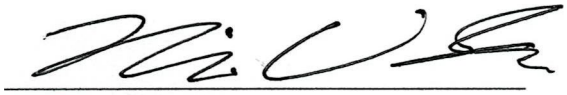
i. In light of the aforementioned, including the facts that demonstrate MARTIN possessed and distributed child pornography, I think (based on my training and experience) that it is highly probable that MARTIN is a child pornography collector.

27. Based on the evidence in this investigation, I believe that MARTIN, likely displays characteristics common to individuals who produce, distribute, receive, possess, and/or access with intent to view child pornography.

CONCLUSION

28. Based upon the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the foregoing criminal violations are located in the DEVICES. Therefore, I request a search warrant for the DEVICES listed in Attachment A, authorizing the seizure of the items described in Attachment B.

Respectfully submitted,



Nicholas Ustach
Special Agent
Homeland Security Investigations

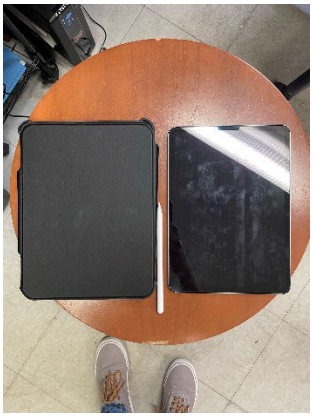
Sworn and subscribed before me this 27th day of June, 2024.

SHON T. ERWIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

ITEMS TO BE SEARCHED

1. Apple iPad with Black Case

2. Apple iPad with Grey Case


3. Blue Motorola Cell Phone

4. Apple iPhone with Grey Case

5. Apple iPhone with Purple Case

6. Apple iPhone with Green Case

7. SanDisk 128 GB SD Card

This warrant authorizes the forensic examination of the DEVICES for the purpose of identifying the electronically stored information described in Attachment B. These items are currently stored at Homeland Security Investigations, Oklahoma City, and located in their secure evidence storage room at 3625 NW 56th St, Oklahoma City, Oklahoma

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. All records on the DEVICES described in Attachment A that relate to violations of Title 18 U.S.C. §§ 2251 and 2252A(possession, distribution, and production of child pornography), and Title 18 U.S.C. § 1591(a)(sex trafficking of children) including:

   A. Any and all evidence of who used, owned, or controlled the DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   B. Any and all evidence indicating how and when the DEVICES were accessed or used to determine the chronological context of DEVICES access, use, and events relating to crimes under investigation and to the DEVICES' user(s);

   C. Any and all evidence indicating the DEVICES' user's state of mind as it relates to the crimes under investigation;

   D. Any and all evidence of the times the DEVICES were used;

   E. Any and all passwords, encryption keys, and other access devices that may be necessary to access the DEVICES;

F. Any and all records of or information about Internet Protocol addresses used by the DEVICES;

G. Any and all records of or information about the DEVICES' internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

H. Any and all contextual information necessary to understand the evidence described in this attachment;

I. Any and all evidence of the violations described above, including communications with children or those purporting to be children, photos or videos of females that might be victims of trafficking, including pornography and erotica, and communications with victims and potential buyers of commercial sex, as well as communications, images, photos, and videos related to sex trafficking;

J. Any and all evidence of any means of force, fraud, coercion and recruiting of sex trafficking victims, including children, to include communications regarding gang affiliations and the purchase or sale of controlled substances, firearms, and other weapons;

K. Any and all records, information, and items relating to any hotels, motels, truck stops, or residences;

L. Any and all records, information, and items relating to online escort advertisements, message boards, social media platforms, or other means of advertising and promoting the commercial sex business;

M. Any and all records, information, and items relating to the acquisition, laundering, or possession of any proceeds related to or derived from commercial sex, and/or records, information, and items relating to other sources of compensation and/or legitimate employment and earnings;

N. Any and all records and information relating to the identity or location of the persons suspected of violating the statutes described above or victims thereof;

O. Any and all digital notes, documents, records, or correspondence pertaining to the possession of child pornography as defined in 18 U.S.C. § 2256(8);

P. Any and all digital images of child pornography as defined in 18 U.S.C. § 2256(8);

Q. Any and all digital notes, documents, records, or correspondence concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography;

R. Any and all digital notes, documents, records, or correspondence concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members;

S. Any and all digital records, documents, invoices and materials that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage;

T. Any and all digital address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8);

U. Any and all records pertaining to how the user of the DEVICES acquired or disseminated any child pornography as defined in 18 U.S.C. § 2256(8); and

V. Any and all records pertaining to a sexual interest in children.

W. Any federal law enforcement officer may perform or assist with the search for the aforementioned items, including representatives of the United States Attorney's Office.

2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they

may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.